Fireware XTM v11.9.3 Release Notes

Supported Devices	XTM 3, 5, 8, 800, 1500, and 2500 Series XTM 25, XTM 26, XTM 1050, XTM 2050 Firebox T10, Firebox M440 XTMv, WatchGuard AP
Fireware XTM OS Build	458203 *(updated 2 October, 2014 for all models except Firebox M440)* *Original Fireware XTM OS v11.9.3: 457845, for all models except Firebox M440* *Firebox M440 Build: 458511*
WatchGuard System Manager Build	457859
Release Notes Revision Date	11 November 2014

Introduction

On October 2, 2014, WatchGuard released updated builds of Fireware XTM OS v11.9.3 to include Mobile VPN with SSL v11.9.3 client software. The original Fireware XTM OS software included v11.9.1 Mobile VPN software. At the same time, we also updated the SSO Exchange Monitor software to correct the version number mentioned in the software installer. If you do not use Mobile VPN with SSL, it is not necessary to update to this later build of Fireware XTM OS because there are no other changes in the software.

WatchGuard is pleased to announce the release of Fireware XTM v11.9.3 and WatchGuard System Manager v11.9.3. This maintenance release that includes several significant enhancements, as well as many bug fixes. Highlights include:

- New, general purpose capability to add any DHCP option (vendor extensions). These configuration parameters are typically required in the setup of VoIP phone systems and increase interoperability with systems from Avaya, Mitel, Shoretel, and NEC, among others.
- Updated default proxy actions to better reflect the needs of modern internet traffic. These updated actions will be applied as the default in any new policies created for HTTP, SMTP, POP3, and FTP proxies.
- Logon Banner and Disclaimer for administrative access to your Firebox or XTM device. This is required for companies that comply with ISO27001 or other similar Information Security Management Systems (ISMS).
- WatchGuard System Manager support for the new Firebox T10 Wireless, Firebox T10 DSL, and Firebox M440 models.

- Several enhancements to improve the reliability and ease-of-setup for VPN tunnels, as well as make it easier to diagnose problems, including:
  - New log messages for Mobile VPN login and logout events
  - Phase 2 Force Key Expiration settings have been changed to improve interoperability with third-party devices
  - SSL hub devices now display information on configured SSL VPN management tunnels
- Fault reports now sent back to WatchGuard to enable WatchGuard engineers to better understand device performance in the field and produce better quality products.
- Support for ZTE MF190 modem, and Access Point Name (APN) in modem configurations to provide more carrier options for modem failover support.
- The Fireware XTM installer and the Web UI now show the location of the OS upgrade file, making it easier for users to step through the upgrade process.
- WatchGuard AP firmware has been updated to 1.2.9.2, with an update to make the AP device easier to reset or reboot.

For more information on bug fixes, see the Enhancements and Resolved Issues section. For more information about the feature enhancements and functionality changes included in Fireware XTM v11.9.3, see the product documentation or review What's New in Fireware XTM v11.9.3.

Before You Begin

Before you install this release, make sure that you have:

- A supported WatchGuard Firebox or XTM device. This device can be a WatchGuard Firebox T10, XTM 2 Series (models 25 and 26 only), 3 Series, 5 Series, 8 Series, 800 Series, XTM 1050, XTM 1500 Series, XTM 2050 device, XTM 2500 Series, Firebox M440, or XTMv (any edition).
- The required hardware and software components as shown below. If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware XTM OS installed on your Firebox or XTM device and the version of WSM installed on your Management Server.
- Feature key for your Firebox or XTM device — If you upgrade your device from an earlier version of Fireware XTM OS, you can use your existing feature key. If you use XTMv, your feature key must be generated with the serial number you received when you purchased XTMv.

Note that you can install and use WatchGuard System Manager v11.9.x and all WSM server components with devices running earlier versions of Fireware XTM v11. In this case, we recommend that you use the product documentation that matches your Fireware XTM OS version.

If you have a new Firebox or XTM physical device, make sure you use the instructions in the *Quick Start Guide* that shipped with your device. If this is a new XTMv installation, make sure you carefully review the *XTMv Setup Guide* for important installation and setup instructions.

Product documentation for all WatchGuard products is available on the WatchGuard web site at www.watchguard.com/help/documentation.

Localization

This release includes localized management user interfaces (WSM application suite and Web UI)current as of Fireware XTM v11.8.UI changes introduced since v11.8 remain in English. Supported languages are:

- Chinese (Simplified, PRC)
- French (France)
- Japanese
- Spanish (Latin American)

Note that most data input must still be made using standard ASCII characters. You can use non-ASCII characters in some areas of the UI, including:

- Proxy deny message
- Wireless hotspot title, terms and conditions, and message
- WatchGuard Server Center users, groups, and role names

Any data returned from the device operating system (e.g. log data) is displayed in English only. Additionally, all items in the Web UI System Status menu and any software components provided by third-party companies remain in English.

Fireware XTM Web UI

The Web UI will launch in the language you have set in your web browser by default.

WatchGuard System Manager

When you install WSM, you can choose what language packs you want to install. The language displayed in WSM will match the language you select in your Microsoft Windows environment. For example, if you use Windows 7 and want to use WSM in Japanese, go to Control Panel > Regions and Languages and select Japanese on the Keyboards and Languages tab as your Display Language.

Dimension, WebCenter, Quarantine Web UI, and Wireless Hotspot

These web pages automatically display in whatever language preference you have set in your web browser.

Fireware XTM and WSM v11.9.3 Operating System Compatibility

Last revised May 2014, with the release of v11.9

WSM/ Fireware XTM Component	Microsoft Windows XP SP2 (32-bit) & Vista (32 &64-bit)	Microsoft Windows 7, 8, 8.1 (32-bit & 64-bit)	Microsoft Windows Server 2003 SP2 (32-bit)	Microsoft Windows Server 2008 & 2008 R2	Microsoft Windows Server 2012 &2012 R2 (64-bit)	Mac OS X v10.6, v10.7, v10.8, v10.9	Android 4.x	iOS v5, v6 & v7
WatchGuard System Manager	✓	✓	✓	✓	✓			
WatchGuard Servers *For information on WatchGuard Dimension, see the [Dimension Release Notes](). *	✓	✓	✓	✓	✓			
Single Sign-On Agent (Includes Event Log Monitor)			✓	✓	✓			
Single Sign-On Client	✓	✓	✓	✓	✓	✓		
Single Sign-On Exchange Monitor[1]			✓[2]	✓	✓			
Terminal Services Agent[3]			✓	✓	✓			
Mobile VPN with IPSec	✓	✓				✓[4]	✓	✓[4]
Mobile VPN with SSL	✓	✓[5]	✓			✓	✓	✓

Notes about Microsoft Windows support:

- *For Microsoft Windows Server 2008, we support both 32-bit and 64-bit support. For Windows Server 2008 R2, we support 64-bit only.*
- *Windows 8.x support does not include Windows RT.*

The following browsers are supported for both Fireware XTM Web UI and WebCenter (Javascript required):

- *IE 9 and later*
- *Firefox v22 and later*
- *Safari 5 and later*
- *Safari iOS 6 and later*
- *Chrome v29 and later*

[1] Microsoft Exchange Server 2003, 2007, and 2010 are supported.

[2] Exchange Monitor is supported on Windows Server 2003 R2.

[3] Terminal Services support with manual or Single Sign-On authentication operates in a Microsoft Terminal Services or Citrix XenApp 4.5, 5.0, 6.0 and 6.5 environment.

[4] Native (Cisco) IPSec client and OpenVPN are supported for Mac OS and iOS. For Mac OS X 10.8 and 10.9, we also support the WatchGuard IPSec Mobile VPN Client for Mac, powered by NCP.

[5] Mobile VPN with SSL is supported on Windows 8.1 with an installation workaround described in this Knowledge Base article.

Authentication Support

This table gives you a quick view of the types of authentication servers supported by key features of Fireware XTM. Using an authentication server gives you the ability to configure user and group-based firewall and VPN policies in your XTM device configuration. With each type of third-party authentication server supported, you can specify a backup server IP address for failover.

✓ *Fully supported by WatchGuard* 🏳 *Not yet supported, but tested with success by WatchGuard customers*

	Active Directory[1]	LDAP	RADIUS[2]	SecurID[2]	Firebox (Firebox-DB) Local Authentication
Mobile VPN with IPSec/Shrew Soft	✓	✓	✓[3]	–	✓
Mobile VPN with IPSec/WatchGuard client (NCP)	✓	✓	✓	✓	✓
Mobile VPN with IPSec for iOS and Mac OS X native VPN client	⚑	⚑	⚑	✓	✓
Mobile VPN with IPSec for Android devices	✓	✓	✓	–	✓
Mobile VPN with SSL for Windows	✓	✓	✓[4]	✓[4]	✓
Mobile VPN with SSL for Mac	✓	✓	✓	✓	✓
Mobile VPN with SSL for iOS and Android devices	⚑	⚑	⚑	✓	✓
Mobile VPN with L2TP	✓[6]	–	✓	–	✓
Mobile VPN with PPTP	–	–	✓	N/A	✓
Built-in Authentication Web Page on Port 4100	✓	✓	✓	✓	✓
Single Sign-On Support *(with or without client software)*	✓	✓	–	–	–
Terminal Services Manual Authentication	✓	⚑	⚑	⚑	✓
Terminal Services Authentication with Single Sign-On	✓[5]	–	–	–	–
Citrix Manual Authentication	⚑	⚑	⚑	⚑	✓
Citrix Manual Authentication with Single Sign-On	✓[5]	–	–	–	–

1. *Active Directory support includes both single domain and multi-domain support, unless otherwise noted.*
2. *RADIUS and SecurID support includes support for both one-time passphrases and challenge/response authentication integrated with RADIUS. In many cases, SecurID can also be used with other RADIUS implementations, including Vasco.*
3. *The Shrew Soft client does not support two-factor authentication.*
4. *Fireware XTM supports RADIUS Filter ID 11 for group authentication.*
5. *Both single and multiple domain Active Directory configurations are supported.For information about the supported Operating System compatibility for the WatchGuard TO Agent and SSO Agent, see the current Fireware XTM and WSM Operating System Compatibility table.*
6. *Active Directory authentication methods are supported only through a RADIUS server.*

System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Minimum CPU	Intel Pentium IV 1GHz	Intel Pentium IV 2GHz
Minimum Memory	1 GB	2 GB
Minimum Available Disk Space	250 MB	1 GB
Minimum Recommended Screen Resolution	1024x768	1024x768

XTMv System Requirements

With support for installation in both a VMware and a Hyper-V environment, a WatchGuard XTMv virtual machine can run on a VMware ESXi 4.1, 5.0 or 5.1 host, or on Windows Server 2008 R2, Windows Server 2012, Hyper-V Server 2008 R2, or Hyper-V Server 2012.

The hardware requirements for XTMv are the same as for the hypervisor environment it runs in.

Each XTMv virtual machine requires 3 GB of disk space.

Recommended Resource Allocation Settings

	Small Office	Medium Office	Large Office	Datacenter
Virtual CPUs	1	2	4	8 or more
Memory	1 GB	2 GB	4 GB	4 GB or more

Downloading Software

To download software:

1. Go to the WatchGuard Software Downloads page.
2. Select the Firebox or XTM device for which you want to download software.

There are several software files available for download. See the descriptions below so you know what software packages you will need for your upgrade.

WatchGuard System Manager

With this software package you can install WSM and the WatchGuard Server Center software:

`WSM11_9_3.exe` — Use this file to upgrade WatchGuard System Manager from v11.x to WSM v11.9.3.

Fireware XTM OS

Select the correct Fireware XTM OS image for your XTM device. Use the .exe file if you want to install or upgrade the OS using WSM. Use the .zip file if you want to install or upgrade the OS using the Fireware XTM Web UI. Use the .ova or .vhd file to deploy a new XTMv device.

If you have…	Select from these Fireware XTM OS packages
XTM 2500 Series	`XTM_OS_XTM800_1500_2500_11_9_3.exe` `xtm_xtm800_1500_2500_11_9_3.zip`
XTM 2050	`XTM_OS_XTM2050_11_9_3.exe` `xtm_xtm2050_11_9_3.zip`
XTM 1500 Series	`XTM_OS_XTM800_1500_2500_11_9_3.exe` `xtm_xtm800_1500_2500_11_9_3.zip`
XTM 1050	`XTM_OS_XTM1050_11_9_3.exe` `xtm_xtm1050_11_9_3.zip`
XTM 800 Series	`XTM_OS_XTM800_1500_2500_11_9_3.exe` `xtm_xtm800_1500_2500_11_9_3.zip`
XTM 8 Series	`XTM_OS_XTM8_11_9_3.exe` `xtm_xtm8_11_9_3.zip`
XTM 5 Series	`XTM_OS_XTM5_11_9_3.exe` `xtm_xtm5_11_9_3.zip`
Firebox M440	`XTM_OS_M440_11_9_3.exe` `firebox_m440_11_9_3.zip`
XTM 330	`XTM_OS_XTM330_11_9_3.exe` `xtm_xtm330_11_9_3.zip`
XTM 33	`XTM_OS_XTM33_11_9_3.exe` `xtm_xtm33_11_9_3.zip`
XTM 2 Series Models 25, 26	`XTM_OS_XTM2A6_11_9_3.exe` `xtm_xtm2a6_11_9_3.zip`
Firebox T10	`XTM_OS_T10_11_9_3.exe` `firebox_T10_11_9_3.zip`

XTMv
All editions for VMware
	`xtmv_11_9_3.ova`
	`xtmv_11_9_3.exe`
	`xtmv_11_9_3.zip`

XTMv
All editions for Hyper-V
	`xtmv_11_9_3_vhd.zip`
	`xtmv_11_9_3.exe`
	`xtmv_11_9_3.zip`

Single Sign-On Software

For Single Sign-On (SSO) capability in a Windows Active Directory Domain. Agent requires the Microsoft .NET Framework v2.0 –4.5 or later. These files are available for Single Sign-On. Several of these files have been updated with this release.

- `WG-Authentication-Gateway_11_9_3.exe` (SSO Agent software - required for Single Sign-On and includes optional Event Log Monitor for clientless SSO)
- `WG-Authentication-Client_11_9_3.msi` (SSO Client software for Windows)
- `WG-SSOCLIENT-MAC_11_8_1.dmg` (SSO Client software for Mac OS X)
- `SSOExchangeMonitor_x86_11_9.exe` (Exchange Monitor for 32-bit operating systems)
- `SSOExchangeMonitor_x64_11_9.exe` (Exchange Monitor for 64-bit operating systems)

For information about how to install and set up Single Sign-On, see the product documentation.

Terminal Services Authentication Software

For User Authentication in Terminal Services or Citrix XenApp Environments.

- `TO_AGENT_SETUP_11_9_3.exe` (This installer includes both 32-bit and 64-bit file support and is updated for this release.)

Mobile VPN with SSL Client for Windows and Mac

There are two files available for download if you use Mobile VPN with SSL. Both clients are updated with this release.

- `WG-MVPN-SSL_11_9_3.exe` (Client software for Windows)
- `WG-MVPN-SSL_11_9_3.dmg` (Client software for Mac)

Mobile VPN with IPSec client for Windows and Mac

There are three available files to download. No clients have been updated with this release.

- `Shrew Soft Client 2.2.0 for Windows` - Shrew Soft has recently released a v2.2.1 client, available on their web site, which introduces a new "Pro" version available at an extra cost with additional features. WatchGuard recommends you use the no-cost Standard version of the client as it includes all functionality supported in the v2.2.0 VPN client. If you want to use the v2.2.1 client, we recommend you read this Knowledge Base article first.
- `WatchGuard IPSec Mobile VPN Client for Windows, powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.
- `WatchGuard IPSec Mobile VPN Client for Mac OS X, powered by NCP` - There is a license required for this premium client, with a 30-day free trial available with download.

WatchGuard AP Firmware

If you manage WatchGuard AP devices and your Gateway Wireless Controller is enabled to update these devices automatically, your AP devices will be upgraded to new firmware when you upgrade your XTM device to XTM OS v11.9.x for the first time. You can also upgrade the AP device software for an individual AP device from the Gateway Wireless Controller.If you want to update your WatchGuard AP devices manually without using the Gateway Wireless Controller, you can open the WatchGuard AP Software Download page and download the latest AP firmware and manually update your AP devices. We also provide the files to manually update the firmware for an unpaired AP device, if required. The file names for the most current AP firmware are:

- `AP100-v1.2.9.2.bin`
- `AP200-v1.2.9.2.bin`

Upgrade Notes

In addition to new features and functionality introduced in Fireware XTM v11.9.x, this release also changes the functionality of several existing features in ways that you need to understand before you upgrade. In this section, we review the impact of some of these changes, as well as highlight several known issues related to upgrading.

- Because many features in Fireware XTM v11.9.x operate very differently than in previous versions and Policy Manager can manage devices that use different versions of Fireware XTM OS, you must now select the Fireware XTM version the device uses before you can configure some features. In Policy Manager, go to **Setup > OS Compatibility** to select a version.
- The Mobile VPN with SSL **Bridge VPN Traffic** option now requires that you first configure a network bridge. When you upgrade to v11.9 or higher, if Mobile VPN with SSL was configured to bridge VPN traffic to an interface, the upgrade process automatically creates a new bridge that includes the interface.
- Previously, you had to associate your wireless interface with your trusted or optional interface (or use the wireless guest network). When you upgrade a network bridge is created that has the trusted or optional interface and the wireless interface as members. After you upgrade, make sure to verify your wireless policies meet the needs of your network. If you use Centralized Management, see this Knowledge Base article for important information about this upgrade.
- Because the redesigned traffic management feature works differently than in previous versions, when you upgrade a configuration from 11.8.x or lower to 11.9 or higher, any existing traffic management actions are removed.

Upgrade from Fireware XTM v11.x to v11.9.3

Before you upgrade from Fireware XTM v11.x to Fireware XTM v11.9.x, download and save the Fireware XTM OS file that matches the WatchGuard device you want to upgrade. You can use Policy Manager or the Web UI to complete the upgrade procedure. We strongly recommend that you back up your device configuration and your WatchGuard Management Server configuration before you upgrade. It is not possible to downgrade without these backup files.

If you use WatchGuard System Manager (WSM), make sure your WSM version is equal to or higher than the version of Fireware XTM OS installed on your XTM device and the version of WSM installed on your Management Server. Also, make sure to upgrade WSM before you upgrade the version of XTM OS on your XTM device.

If you use an XTM 5 Series or 8 Series device, you must upgrade to Fireware XTM v11.7.4 or v11.7.5 before you can upgrade to Fireware XTM v11.9.x.

We recommend that you reboot your XTM device before you upgrade. While this is not necessary for most higher-model XTM devices, a reboot clears your XTM device memory and can prevent many problems commonly associated with upgrades in XTM 2 Series, 3 Series, and some 5 Series devices.

Back up your WatchGuard Servers

It is not usually necessary to uninstall your previous v11.x server or client software when you update to WSM v11.9.x. You can install the v11.9.x server and client software on top of your existing installation to upgrade your WatchGuard software components. We do, however, strongly recommend that you back up your WatchGuard Servers (for example: WatchGuard Log Server, WatchGuard Report Server, or WatchGuard Dimension Log Server) before you upgrade. You need these backup files if you ever want to downgrade.

To back up your Management Server configuration, from the computer where you installed the Management Server:

1. From WatchGuard Server Center, select **Backup/Restore Management Server**.
   The WatchGuard Server Center Backup/Restore Wizard starts.
2. Click **Next**.
   The Select an action screen appears.
3. Select **Back up settings**.
4. Click **Next**.
   The Specify a backup file screen appears.
5. Click **Browse** to select a location for the backup file. Make sure you save the configuration file to a location you can access later to restore the configuration.
6. Click **Next**.
   The WatchGuard Server Center Backup/Restore Wizard is complete screen appears.
7. Click **Finish** to exit the wizard.

Upgrade to Fireware XTM v11.9.x from Web UI

1. Go to **System > Backup Image** or use the USB Backup feature to back up your current device image.
2. On your management computer, launch the OS software file you downloaded from the WatchGuard Software Downloads page.
   If you use the Windows-based installer on a computer with a Windows 64-bit operating system, this installation extracts an upgrade file called *[xtm series]_[product code].sysa-dl* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.9\[model] or [model][product_code].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.9
3. Connect to your XTM device with the Web UI and select **System > Upgrade OS**.
4. Browse to the location of the *[xtm series]_[product code].sysa-dl* from Step 2 and click **Upgrade**.

Upgrade to Fireware XTM v11.9.x from WSM/Policy Manager v11.x

1. Select **File > Backup** or use the USB Backup feature to back up your current device image.
2. On a management computer running a Windows 64-bit operating system, launch the OS executable file you downloaded from the WatchGuard Portal. This installation extracts an upgrade file called *[xtm series]_[product code].sysa-dl* l to the default location of C:\Program Files(x86)\Common files\WatchGuard\resources\FirewareXTM\11.9\[model] or [model][product_code].
   On a computer with a Windows 32-bit operating system, the path is: C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.9
3. Install and open WatchGuard System Manager v11.9.3. Connect to your XTM device and launch Policy Manager.
4. From Policy Manager, select **File > Upgrade**. When prompted, browse to and select the *[xtm series]_[product code].sysa-dl* file from Step 2.

Upgrade your FireCluster to Fireware XTM v11.9.x

There are two methods to upgrade Fireware XTM OS on your FireCluster. The method you use depends on the version of Fireware XTM you currently use.

> If you use an XTM 5 Series or 8 Series device, you must upgrade your FireCluster to Fireware XTM v11.7.4 or v11.7.5 before you can upgrade your FireCluster to Fireware XTM v11.9.x.

> We recommend that you use Policy Manager to upgrade, downgrade, or restore a backup image to a FireCluster. It is possible to do some of these operations from the Web UI but, if you choose to do so, you must follow the instructions in the Help carefully as the Web UI is not optimized for these tasks. It is not possible to upgrade your FireCluster from v11.8.x to v11.9.x with the Web UI.

Upgrade a FireCluster from Fireware XTM v11.4.x–v11.8.x to v11.9.x

Use these steps to upgrade a FireCluster to Fireware XTM v11.9.x:

1. Open the cluster configuration file in Policy Manager
2. Select **File > Upgrade**.
3. Type the configuration passphrase.
4. Type or select the location of the upgrade file.
5. To create a backup image, select **Yes**.
   A list of the cluster members appears.
6. Select the check box for each device you want to upgrade.
   A message appears when the upgrade for each device is complete.

When the upgrade is complete, each cluster member reboots and rejoins the cluster. If you upgrade both devices in the cluster at the same time, the devices are upgraded one at a time. This is to make sure there is not an interruption in network access at the time of the upgrade.

Policy Manager upgrades the backup member first and then waits for it to reboot and rejoin the cluster as a backup. Then Policy Manager upgrades the master. Note that the master's role will not change until it reboots to complete the upgrade process. At that time the backup takes over as the master.

To perform the upgrade from a remote location, make sure the FireCluster interface for management IP address is configured on the external interface, and that the management IP addresses are public and routable. For more information, see About the Interface for Management IP Address.

Upgrade a FireCluster from Fireware XTM v11.3.x

To upgrade a FireCluster from Fireware XTM v11.3.x to Fireware XTM v11.9.x, you must perform a manual upgrade. For manual upgrade steps, see the Knowledge Base article Upgrade Fireware XTM OS for a FireCluster.

Downgrade Instructions

Downgrade from WSM v11.9.x to WSM v11.x

If you want to revert from v11.9.x to an earlier version of WSM, you must uninstall WSM v11.9.x. When you uninstall, choose **Yes** when the uninstaller asks if you want to delete server configuration and data files. After the server configuration and data files are deleted, you must restore the data and server configuration files you backed up before you upgraded to WSM v11.9.x.

Next, install the same version of WSM that you used before you upgraded to WSM v11.9.x. The installer should detect your existing server configuration and try to restart your servers from the **Finish** dialog box. If you use a WatchGuard Management Server, use WatchGuard Server Center to restore the backup Management Server configuration you created before you first upgraded to WSM v11.9.x. Verify that all WatchGuard servers are running.

Downgrade from Fireware XTM v11.9.x to Fireware XTM v11.x

> ⚠ If you use the Fireware XTM Web UI or CLI to downgrade from Fireware XTM v11.9.x to an earlier version, the downgrade process resets the network and security settings on your XTM device to their factory-default settings. The downgrade process does not change the device passphrases and does not remove the feature keys and certificates.

If you want to downgrade from Fireware XTM v11.9.x to an earlier version of Fireware XTM, the recommended method is to use a backup image that you created before the upgrade to Fireware XTM v11.9.x. With a backup image, you can either:

- Restore the full backup image you created when you upgraded to Fireware XTM v11.9.x to complete the downgrade; or
- Use the USB backup file you created before the upgrade as your auto-restore image, and then boot into recovery mode with the USB drive plugged in to your device. This is not an option for XTMv users.

See the *WatchGuard System Manager Help* or the *Fireware XTM Web UI Help* for more information about these downgrade procedures, and information about how to downgrade if you do not have a backup image.

Downgrade Restrictions

Some downgrade restrictions apply:

- You cannot downgrade an XTM 2050 or an XTM 330 to a version of Fireware lower than v11.5.1.
- You cannot downgrade an XTM 25, 26, or 33 device to a version of Fireware lower than v11.5.2.
- You cannot downgrade an XTM 5 Series model 515, 525, 535 or 545 to a version of Fireware lower than v11.6.1.
- You cannot downgrade a Firebox T10 to a version of Fireware lower than v11.8.3.
- You cannot downgrade a Firebox M440 to a version of Fireware lower than v11.9.2.
- You cannot downgrade XTMv in a VMware environment to a version of Fireware lower than v11.5.4.
- You cannot downgrade XTMv in a Hyper-V environment to a version of Fireware lower than v11.7.3.

When you downgrade the Fireware XTM OS on your XTM device, the firmware on any paired AP devices is not automatically downgraded. We recommend that you reset the AP device to its factory-default settings to make sure that it can be managed by the older version of Fireware XTM OS.

Enhancements and Resolved Issues

General

- An issue has been resolved that caused high CPU utilization by the snmpd process. *[80943, 81361]*
- The CPU temperature range used by the hardware monitor was increased to match the recommended temperature range for the CPU in each Firebox or XTM model. This prevents invalid hardware monitor alarms. *[81255]*
- This release resolves a crash in the SNMP process. *[81220]*
- You can now show Gateway AV and IPS signatures through the SNMP MIB OID. *[66396]*
- This release updates the default trusted CA certificate bundle to match that of common web browsers. *[80374]*
- You can now import PKCS#7 format certificates and certificate chains with Firebox System Manager. *[56480]*

WatchGuard System Manager

- When you use WatchGuard System Manager v11.9.x Management Server to create a template that includes the configuration of an Active Directory Authentication Server, you can now apply the template to any Firebox or XTM device running any version of Fireware or Fireware XTM OS earlier than v11.9.x. *[80998]*
- Quarantine email notification messages are correctly localized. *[73036]*
- The Audit trail logging option is now available in Centralized Management Device Templates. *[69484]*
- The scheduled daily PDF report from WatchGuard System Manager Report Server no longer adds HeiseiKakuGo-WS font to the English only report, which allows for successful printing of the report. *[81801]*
- Firebox System Manager > Traffic Monitor now correctly displays log messages that include German umlauts. *[81683]*

Web UI

- PFS is no longer enabled by default for branch office VPN tunnels in the Web UI. *[81491]*
- Static NAT entries now display correctly in the policy list. *[80992, 80936]*
- You can now clone a Traffic Management action in the Fireware XTM Web UI. *[78527]*
- The System Status > Authentication List is no longer black after a user authenticates to the hotspot login page. *[81582]*
- Policy ordering is now the same in both the Web UI and Policy Manager when using an alias or non-default interface name. *[74657]*
- Branch office VPN tunnels configured with the Management Server are now correctly disabled in a Centralized Management installation. *[80850]*
- The connection rate per policy setting now works correctly when configured in the Web UI. *[81858]*
- The Web UI now supports UTF-8 characters in hotspot custom pages. *[81629]*

Authentication

- All Fireware XTM Windows sub-components now include a recovery method. *[81299]*
- The TO Agent now correctly handles partial commands. *[81136]*
- An issue that caused a redirect loop with the hotspot acceptance page has been resolved. *[79699]*
- This release provides better support for RDP login when using the SSO client. *[81519, 81134]*
- Event Log Monitor has been updated with improved cache logic to prevent incorrect logoff status. *[80565]*
- Logon type 7 (Unlock) is now supported for SSO authentication using Event Log Monitor. *[77972]*
- The SSO Port Tester now supports host addresses with 0 or 255 as the last octet. *[78601]*
- You can now download SSO components diagnostic log files in the SSO Agent Configuration Tool. *[80504]*
- Event Log Monitor no longer consumes high bandwidth for authentication event checking. *[81913]*

Proxies

- When you configure an FTP Proxy policy for 1-to-1 NAT traffic, the FTP login and data transfer now work correctly. *[77218]*
- When you use the HTTPS proxy with content inspection enabled, connections now work correctly when the Firebox or XTM device has an expired CA certificate with the same name as the active CA certificate for the site. *[81814]*
- A memory corruption issue that prevented the capture of proxy crash log messages has been resolved. *[81353]*
- Traffic management now works correctly for an FTP client in active mode. *[78568]*
- A memory leak has been resolved that occurred when using the SMTP proxy with TLS encryption enabled and an encryption rule configured with the **Server Encryption** set to **Required** and **Recipient Encryption** set to **None**. *[81855]*
- You can now select Deny or Block as actions in the HTTP Proxy Request Header configuration. *[81622]*
- Proxy error log messages have been updated to include helpful information instead of `pxy Unknown notification type='0x2000003'`. *[81841]*
- The Idle Timeout setting is no longer enforced for sites configured as HTTP proxy exceptions. *[77675]*
- The default HTTP Proxy Exception list has been updated to include all domains used for Windows Updates. *[76186]*
- The POP3 proxy now strips incorrectly formatted message headers to prevent an issue that made the Thunderbird email client unable to correctly display email messages. *[80016]*
- Mail delivery no longer fails when TLS is enabled for the SMTP proxy and encryption is configured as optional-preferred. *[79344]*
- This release resolves an issue in which H.323 calls caused the proxy worker process to crash. *[78585]*
- This release resolves an issue that caused the per policy QoS settings on the H.323 and SIP ALGs to reset to zero after making any change in diagnostic log settings. *[81296]*

Security Subscription Services

- A memory leak has been fixed in the Gateway AV scanning process. *[81244]*
- An issue that caused the Gateway AV scanning process to fail has been resolved. *[81544]*
- Gateway AV scans no longer identify the Adobe FlashPlayer download as the virus `Luhe.Packed.C`. *[81018]*
- IPS now scans the data channel of FTP connections. *[80557]*
- This release resolves a kernel crash that occurred when using IPS or Application Control. *[79530]*

- Several issues that caused the spamBlocker process to crash under stress has been resolved. *[77856, 79624, 81108]*
- WebBlocker now correctly processes invalid WebBlocker requests. *[81153]*
- Email notifications for WebBlocker now include the user name if the user has authenticated. *[55979]*
- The delay in web site loading when the WebBlocker server is unavailable and access to the website is allowed has been decreased. *[71223]*
- You can now select WebBlocker parent categories independently of the sub categories when using Websense. *[79630]*
- This release resolves an issue that caused all traffic to fail through policies using WebBlocker after a configuration change to the WebBlocker settings with a proxy traffic log message `error="No profile found for name.` *[81554]*
- The DLP Activity summary report no longer fails to complete. *[81667]*
- Log messages for security subscriptions services have been improved to allow for time slice reporting. *[81351]*

Networking

- If you use multi-WAN configured in round-robin, interface overflow, or failover mode together with a hotspot associated with an interface configured as a LAN bridge, hotspot traffic now correctly passes through that interface after you upgrade to Fireware XTM v11.9.x. *[80532]*
- If your device is configured in bridge mode, the default packet handling feature to Drop IP Source Route attacks now works correctly. *[79653]*
- This release fixes several crashes that occurred when running the XTM device in Bridge mode. *[81399, 81400]*
- Download speed is no longer significantly reduced when you use the Outgoing Interface Bandwidth feature on a trusted interface, *[80783]*
- The Firebox or XTM device now correctly obtains an external IP address with DHCP when its gateway is on a different subnet than the assigned external IP address. *[81527]*
- A modem connection now correctly re-establishes when the modem loses cellular connection or the connection is dropped from 4G to 3G or lower. *[81573, 86611]*
- When the external interface is configured with DHCP and as part of a multi-WAN configuration, it now operates correctly after a ping probe fails, then succeeds. *[81573]*
- The Server Load Balancing Sticky Connection timer is no longer reset after a configuration save. *[56873]*
- You can now configure multi-cast over BOVPN when the input interface is configured for Bridge or VLAN. *[79859]*
- The “next-server flag” is now set correctly when using DHCP. *[82057]*
- This release resolves an issue that prevented some websites from loading correctly through an active/active FireCluster configured with the HTTP proxy and multi-WAN in round-robin mode. *[79822]*

VPN

- You can now configure the Management Server to exclude IPSec certificates as the preferred authentication option for VPN tunnels and instead restrict the authentication method to shared keys. This prevents unnecessary certificate creation and preserves bandwidth for devices that will not use a certification for BOVPNs. *[80994]*
- When you use the v11.9.1 Mobile VPN with SSL client to connect with a Mac client system, you can now resolve VPN network resources by DNS name. *[81529]*
- When a Firebox or XTM device is configured with multiple external interfaces, Mobile VPN with PPTP sessions now connect correctly. *[81585, 81498]*

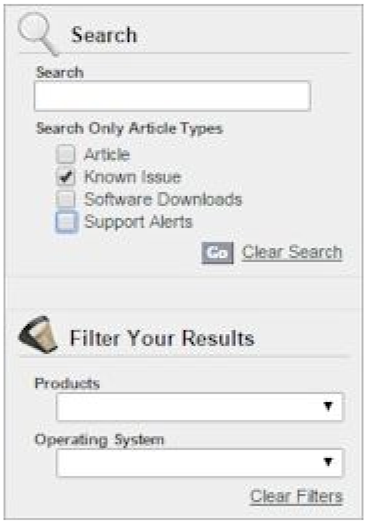
- A path MTU issue that prevented traffic from successfully passing through a zero route branch office VPN tunnel has been resolved. *[77129]*
- An issue has been resolved that prevented traffic from passing through proxy policies on a central site when traffic was generated from a remote site through a zero route branch office VPN tunnel using 1-to-1 NAT. *[81006]*
- ECMP now works correctly with two Virtual Interface BOVPN tunnels. *[81158]*
- This release resolves an issue that prevented PPTP connections from working correctly with a device configured to use multi-WAN. *[81585]*
- The default setting for Branch Office VPN Phase 2 Force Key Expiration has been updated to rekey only based on time. *[74937]*
- This release resolves an issue that prevented SSLVPN connections after a FireCluster failover event occurred. *[76878]*
- Traffic now routes through the correct branch office VPN tunnel, when the tunnel is configured with 1-to-1 NAT in a multi-WAN environment when the interface used for the VPN was not included in the multi-WAN load balancing configuration. *[80389]*

XTM Wireless and WatchGuard AP

- An issue has been resolved that caused XTM wireless connections to fail when Rogue AP detection was enabled. *[77716]*
- An issue has been resolved that caused XTM wireless connections to fail with the log message `ath; phy0: Failed to stop TX DMA.` *[75254]*
- The Site Survey operation now correctly completes with no WatchGuard AP device reboot required. *[71944]*
- This release resolves an issue with Gateway Wireless Controller that caused AP status to frequently change between Discovered and Offline. *[82017]*

Known Issues and Limitations

You can find information about known issues for Fireware XTM v11.9.3 and its management applications, including workarounds where available, in the WatchGuard Knowledge Base. You must log in to the WatchGuard Portal to search for Known Issues. Known Issues are not available in the public version of the Knowledge Base. After you log in, you can use the filters available in the WatchGuard Portal > Knowledge Base tab to find articles about known issues for this release.



Search Only Article Types

- ☐ Article
- ☑ Known Issue
- ☐ Software Downloads
- ☐ Support Alerts

Using the CLI

The Fireware XTM CLI (Command Line Interface) is fully supported for v11.x releases. For information on how to start and use the CLI, see the *CLI Command Reference Guide*. You can download the latest CLI guide from the documentation web site at http://www.watchguard.com/help/documentation/xtm.asp.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or log in to the WatchGuard Portal on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375